during an export operation, encrypting the textual value of each private configuration variable or, during an import operation, decrypting the textual value of each private configuration variable during an import operation;

during an export operation, for each configuration variable, deriving the textual value from the memory value of the configuration variable or, during an import operation, deriving the memory value from the textual value of the configuration variable and updating the corresponding values of the configuration variable; and

during an export operation, receiving the data password and a file name of the persistent configuration text file, hashing the data password into a textual hashed digest, writing the textual hashed digest to the persistent configuration text file, and for each configuration variable, receiving the textual identifier and the textual value, writing the textual identifier and the textual value to the persistent configuration text file, and textually associating the memory identifier and the textual value in the persistent configuration text file.

REMARKS

The new claims generally reflect method and computer product counterparts to the apparatus claims allowed in the parent case. New Claims 8-9 and 13-14 correspond to Claims 8 and 9 in the parent case (which were added during prosecution). New Claims 10-12 and 15-17 correspond to Claims 1-3 in the parent case as amended during prosecution.

Respectfully submitted,

Steven R. Ormiston
Attorney for Applicants
Reg. No. 35,974
(208) 433-1991

VERSION WITH MARKINGS TO SHOW CHANGES

Amendments To The Specification

a. The paragraph beginning on page 5, line 11:

FIG. 1 shows a simplified representation of a memory-base configuration variable table. Each row represents a memory configuration variable, each column represents an attribute of the variable thus identified. The memory identifier column 350 contains a value for identifying the configuration variable to the server. The memory value column 355 contains the current value of the identified variable. The private or public flag column 360 distinguishes private data from public data. In FIG. 1, the data enclosed in brackets in memory column 355 denotes a binary representation of sample data, the data enclosed in quotation marks denotes the clear text representation of the binary data. The private or public column 360 is used primarily to distinguish private data that is to be encrypted before being written to a configuration file from public data, written in clear-text form. The preferred embodiment uses [SNMP] Simple Network Management Protocol (SNMP) [4] object identifiers for the memory identifiers 350. In the preferred embodiment, user passwords, the SNMP get community name, and the SNMP set community name are private data. The remaining configuration data is public. In the preferred embodiment the configuration variable table 345 illustrated in FIG. 1 is implemented logically as described, although some of the columns are implicit. In particular, the private or public column 360 is implicitly by code logic rather than an explicit table entry.

b. The paragraph beginning on page 6, line 11:

FIG. 3 is a block diagram that generally shows the preferred embodiment. The perferred embodiment is generally implemented as the ExtendNet VPN 1000 [2], a commercial product. The ExtendNet VPN includes both a [discrete VPN] discrete Virtual Private Network (VPN) server and a server management utility commercially known as InterprEYES. In the preferred embodiment, the server 600

. is a [vpn] VPN server.

c. The paragraph beginning on page 6, line 16:

The configuration variable table 345 of the preferred embodiment contains numerous variables including general configuration variables such as the system name, the system contact, the system level, a trace level for debug purposes, the admin console [ip] IP address, the admin console IPX network, and the admin console IPX node. The configuration variable table 345 in the preferred embodiment also contains a network configuration section, including a user authentication code, and a packet compression bitmask. The configuration variable table 345 in the preferred embodiment also contains a variable for each user having permission to use the VPN. Each user configuration variable includes a user name, user password, a web access flag, and an account disabled flag. The configuration variable table 345 in the preferred embodiment also contains a server TCP/IP configuration section, including an IP address, a subnet mask, a default gateway, a connection timeout checking flag, a firmware update TFTP port, and a boot protocols section variable. The configuration variable table 345 in the preferred embodiment also contains a client TCP/IP configuration section including a client TCP/IP enable flag, a client-to-client communication flag, and address source variable to indicate whether client [ip] IP address come from an internal table or form a DHCP server, the primary DNS server IP address, the secondary DNS server IP address, the primary NetBios name server IP address, [the] and the secondary NetBios name server IP address[,]. The configuration variable table 345 in the preferred embodiment also contains an IPX configuration section including an IPX enable flag, an LPX frame format variable, a SAP interval variable, a client enable flag, a client network number variable, and a client-to-client communication flag. The configuration variable table 345 in the preferred 15 embodiment also contains SNMP configuration section including the trap community name, the get community name, and the set community name. The configuration variable table 345 in the preferred

embodiment also contains a trap configuration section including an urgent traps bitmask, a warning traps lists, an information traps list, and a debug traps list.

d. The paragraph beginning on page 6, line 16:

In the preferred embodiment, the encryption/decryption apparatus 610 is a software routine deploying well known encryption algorithm [DES] Data Encryption Standard (DES) [4], and the encryption key is the data password 550. The server configuration import/export apparatus 620 is a software routine that resides within the server 600. The server configuration import/export apparatus 620 is an SNMP [4] handler, which responds to read/write requests for individual SNMP variables, each SNMP variable is defined by an object identifier descripter (OID). During an export, upon a proper request via the SNMP interface [570], the server configuration import/export apparatus 620 receives an SNMP request containing an OID corresponding to a memory identifier 350 of the configuration variable table 345. The corresponding memory identifier 350 and the corresponding textual value 375 are wrapped in an SNMP packet and transmitted via SNMP to the client import/export apparatus 525. The public variables are transmitted in clear text; the private variables are encrypted by the encryption/decryption apparatus 610, which is a software implementation of the well known 56 bit DES encryption algorithm. As a security measure, private data is returned via SNMP only if the server 600 is put into a private data manipulation mode via a special SNMP call. Thus, if a general SNMP client will not be able to retrieve any private data, (even though the data would be encrypted), private data transmission is intended to be limited to the server management program 520.

e. The paragraph beginning on page 8, line 21:

In the preferred embodiment, the server password 540 is a SNMP get/set community name pair and the data password 550 is arbitrarily chosen by an authenticated system administrator 500 at the time of an export.

f. The paragraph beginning on page 9, line 1:

The client configuration [inport/export] import/export apparatus 525 also can optionally contain a mechanism to selectively prohibit the restoration of certain variables. This mechanism is useful in situations where a full restore would change system variables such as server passwords and addresses that are [preferable] preferably left unchanged in some restorations. The mechanism typically consists of an internal table and a menu means for the system administrator 500 to identify the variables to be excluded from a restore. The table is then applied against each variable prior to it being sent to the server 600, those variables within the table are not transmitted.

g. The paragraph beginning on page 9, line 11:

Referring to FIG. 3, to save a persistent configuration text file 5 *1* 0, a system administrator 500 executes the server management program 520. The system administrator 500 must present the server password 540 to authenticate to the server 600, which in the preferred embodiment is a [vpn] VPN server. Once authenticated, the system administrator 500 then invokes the save/restore configuration control apparatus 530 of the server management program 520. The system administrator 500 provides a data password 550 and a file name for the persistent configuration text file 510. In the preferred embodiment, the data password 550 [servers] serves both as an encryption/decryption key. The save request is transmitted to the configuration import/export apparatus 620 of the [vpn]

VPN server 600 via the SNMP protocol. The server configuration import/export apparatus 610 then initiates an export. The textual value 375 for each private variable is computed by encrypting the plain-text value 355 within the server 600 into an encrypted textual value 375 using the encryption/decryption apparatus 610 using an encryption key derived from the data password 550. In the preferred embodiment, the encryption/decryption apparatus 610 is a software routine deploying well known encryption algorithm DES, and the encryption key is the data password 550.

h. The paragraph beginning on page 10, line 4:

In the preferred embodiment, the client configuration import/export apparatus 525 performs the following steps when export is selected. First, the system administrator 500 is prompted via a dialog box to enter the data password 500, then prompted to re-enter the passwords for verification. Next, the system administrator 500 is prompted to enter the [export file] configuration file 510 name. The export file is opened for output. An MD4 hash digest signature of the data password 550 is written to the configuration file 510 in a textual form. The client/configuration import/export apparatus 525 contains a number of internal tables, each internal table corresponding to each section within the persistent text file 510. Each table entry consists of an SNMP object identifier descriptor (OID), a data type, and a list of enumeration constants.

i. The paragraph beginning on page 10, line 14:

As a security measure, the SNMP interface, by default, will allow private data to be read or written (even though private data, when returned, is encrypted). The client configuration import/export apparatus sends a special SNMP call to turn on private data manipulation. After the export is complete an analogous SNMP call turns off private data manipulation.

j. The paragraph beginning on page 10, line 19:

Private data manipulation is turned on. Code for each table is invoked. For each section, section headers are written. For each variable in each table, an SNMP request call containing the [oid] OID of the variable is issued. When the data is returned, the data type and the enumeration constants are used to format the response into a suitable format. After formatting, each variable is written to the [export file] configuration file 510. Each variable is written to the configuration file 510 using the textual identifier 370, followed by an equal sign, followed by the textual value 375, in a file format similar to Windows INI files. After the final section is written, the [export file] configuration file 510 is closed, and private data retrieval is turned off.

k. The paragraph beginning on page 11, line 4:

A configuration variable table 345 is restored analogously to the way it is saved. To restore a file on the same or different server 600, the system administrator 500 must first authenticate to the target server 600 by providing the server password 540 to the server 600 using the server management program 520. A restore command is issued through the server management program 520 via a menu command. The administrator 500 must then present the file name of the persistent configuration text file 510 and the data password 550, which in the preferred embodiment also serves as the decryption key. In the preferred embodiment the encryption key, decryption key, and the data password 550 are identical but in general for some encryption/decryption methods they need not be, as long as the encryption key and the decryption key can be derived from the data password 550. The save/restore configuration control apparatus hashes the data password 550 provided by the system administrator 500 into a digest form (using MD4 in the preferred embodiment) and compares this new digest against the digest in the configuration file 510. If the digests match, the system administrator 500

has entered the proper data password 550 and is authenticated and thus can import all the configuration data, including the private data. If the digests do not match, the administrator 500 is not authenticated to the data in the persistent configuration text file 510, and thus can only import memory values in sets that have no private variables. In the preferred embodiment, the non-data authenticated system administrator can import neither user names nor passwords. If the system administrator 500 is authenticated to the data, the data password 550 is transmitted to the encryption/decryption apparatus 610 of the server configuration import/export apparatus 620 by a special SNMP call.

I. The paragraph beginning on page 12, line 3:

In the preferred embodiment, a section of the persistent configuration text file 510 is processed at a time. The section header is used to locate the corresponding internal section table. Variable data for that section is read from the persistent configuration text file 510. The save/restore configuration control apparatus 530 validates that the particular variable belongs to the section. The save/restore configuration control apparatus 530 formats the value received from the persistent configuration text file 510 using the data type and enumeration constants from its internal tables into a [fOormat] format suitable for SNMP transmission and transmits the [oid] OID and the formatted value to the server configuration import/export apparatus 620. The encryption/decryption apparatus 610 of the server 600 decrypts the private data, and the server configuration import/export apparatus 620 updates the configuration variable table 345 to complete the restore operation. In the case of a system administrator that fails to authenticate with the data password 550, the save/restore configuration control apparatus 530 will refrain from sending any variables sets having encrypted data.

m. The paragraph beginning on page 13, line 10:

The preferred embodiment as show in FIG. [3is] 3 is based on the client server model where the functionality is split between a client computer and a server computer. An alternate embodiment is shown in FIG. 4. In this embodiment, the invention is illustrated in a single device context. In this alternate embodiment, a single device configuration apparatus 526, contained within the server management program 520, replaces the client import/export apparatus 525 and the server configuration import/export apparatus 620 of FIG. 3 and operates on a configuration variable table 345 which generally is a software device that operates on the same computing device as the server management program 520. Alternately, the configuration variable table 345 is contained with a discrete, separate device, connected to the device configuration import/export apparatus 526 through any standard computer connectivity mechanism such as serial port, a bus interface, a network, a parallel port, and infrared or other wireless connection and the like.